**Учебный предмет: «Адаптивные информационные коммуникативные технологии»**

**Преподаватель: Банзаракцаева Оюна Данзановна**

**1. Ребята, письменно законспектировать лекцию.**

**09.12.2022 - Лекция «Защита информации,**

**антивирусная защита»**

***Защита информации –*это применение различных средств и методов, использование мер и осуществление мероприятий для того, чтобы обеспечить систему надежности передаваемой, хранимой и обрабатываемой информации.**

Проблема защиты информации в системах электронной обработки данных возникла практически одновременно с их созданием. Ее вызвали конкретные факты злоумышленных действий над информацией.

Если в первые десятилетия активного использования ПК основную опасность представляли хакеры, подключившиеся к компьютерам в основном через телефонную сеть, то в последнее десятилетие нарушение надежности информации прогрессирует через программы, компьютерные вирусы, глобальную сеть Интернет.

Имеется достаточно много способов несанкционированного доступа к информации, в том числе: просмотр; копирование и подмена данных; ввод ложных программ и сообщений в результате подключения к каналам связи; чтение остатков информации на ее носителях; прием сигналов электромагнитного излучения и волнового характера; использование специальных программ.

**1. Средства опознания и разграничения доступа к информации**

**Одним из наиболее интенсивно разрабатываемых направлений по обеспечению безопасности информации является идентификация и определение подлинности документов на основе электронной цифровой подписи.**

**2. Криптографический метод защиты информации**

**Наиболее эффективным средством повышения безопасности является криптографическое преобразование.**

**3. Компьютерные вирусы**

[***Компьютерный вирус***](https://studopedia.ru/14_114817_kompyuternie-virusi.html)***–*это специально написанная программа, способная самопроизвольно присоединяться к другим программам (заражать их), создавать свои копии и внедрять их в файлы,** системные области компьютера и другие объединенные с ним компьютеры в целях нарушения нормальной работы программ, порчи файлов и каталогов, а также создания разных помех при работе на компьютере.

**Появление вирусов в компьютере определяется по следующим наблюдаемым признакам:**

- уменьшение производительности работы компьютера;

- невозможность и замедление загрузки ОС;

- повышение числа файлов на диске;

- замена размеров файлов;

- периодическое появление на экране монитора неуместных сообщений;

- уменьшение объема свободной ОП;

- резкое возрастание времени доступа к [жесткому диску](https://studopedia.ru/2_74868_zhestkiy-disk.html);

- разрушение файловой структуры;

- загорание сигнальной лампочки дисковода, когда к нему нет обращения.

Основными путями заражения компьютеров вирусами обычно служат съемные диски (дискеты и CD-ROM) и компьютерные сети. Заражение жесткого диска компьютера может произойти в случае загрузки компьютера с дискеты, содержащей вирус.

По тому, какой вид среды обитания имеют вирусы, их классифицируют на загрузочные, файловые, системные, сетевые и файлово – загрузочные (многофункциональные).

[*Загрузочные вирусы*](https://studopedia.ru/8_64914_zagruzochnie-virusi.html)внедряются в загрузочный сектор диска или в сектор, который содержит программу загрузки системного диска.

[*Файловые*](https://studopedia.ru/9_166478_faylovie-virusi.html)*вирусы*помещаются в основном в исполняемых файлах с расширением .СОМ и .ЕХЕ.

*Системные вирусы*внедряются в системные модули и драйверы периферийных устройств, таблицы размещения файлов и таблицы разделов.

*Сетевые вирусы*находятся в компьютерных сетях, а *файлово-загрузочные –*заражают загрузочные секторы дисков и файлы прикладных программ.

По пути заражения среды обитания вирусы разделяются на резидентные и нерезидентные.

*Резидентные вирусы*при заражении компьютера оставляют в ОП свою резидентную часть, которая после заражения перехватывает обращение ОС к другим объектам заражения, внедряется в них и выполняет свои разрушительные действия, которые могут привести к выключению или перезагрузке компьютера. *Нерезидентные вирусы*не заражают ОП компьютера и проявляют активность ограниченное время.

Особенность построения вирусов влияет на их проявление и функционирование.

*Логическая бомба*является программой, которая встраивается в большой программный комплекс. Она безвредна до наступления определенного события, после которого реализуется ее логический механизм.

*Программы-мутанты,*самовоспроизводясь, создают копии, явно отличающиеся от оригинала.

*Вирусы-невидимки,*или стелс-вирусы, перехватывают обращения ОС к пораженным файлам и секторам дисков и подставляют вместо себя незараженные объекты. Эти вирусы при обращении к файлам применяют достаточно оригинальные алгоритмы, позволяющие «обманывать» резидентные антивирусные мониторы.

*Макровирусы*используют возможности макроязыков, которые встроены в офисные программы обработки данных (текстовые редакторы, электронные таблицы).

По степени воздействия на ресурсы компьютерных систем и сетей, или по деструктивным возможностям, выделяют безвредные, неопасные, опасные и разрушительные вирусы.

*Безвредные вирусы*не оказывают патологического влияния на работу компьютера. *Неопасные вирусы*не разрушают файлы, однако уменьшают свободную дисковую память, выводят на экран графические эффекты. *Опасные вирусы*часто вызывают значительные нарушения в работе компьютера. *Разрушительные вирусы*могут привести к стиранию информации, полному или частичному нарушению работы прикладных программ. Важно иметь в виду, что любой файл, способный к загрузке и выполнению кода программы, является потенциальным местом, где может помещаться вирус.

**4. Антивирусные программы**

**Широкое распространение компьютерных вирусов привело к разработке антивирусных программ, которые позволяют обнаруживать и уничтожать вирусы, «лечить» пораженные ресурсы.**

Основой работы большинства антивирусных программ является принцип поиска сигнатуры вирусов. *Вирусной сигнатурой*называют некоторую уникальную характеристику вирусной программы, выдающую присутствие вируса в компьютерной системе.

По способу работы антивирусные программы можно разделить на фильтры, ревизоры, доктора, детекторы, вакцины и др.

*Программы-фильтры –*это «сторожа», которые постоянно находятся в ОП. Они являются резидентными и перехватывают все запросы к ОС на выполнение подозрительных действий, т. е. операций, которые используют вирусы для своего размножения и порчи информационных и программных ресурсов в компьютере, в том числе для переформатирования жесткого диска. Среди них можно выделить попытки изменения атрибутов файлов, коррекции исполняемых СОМ– или ЕХЕ-файлов, записи в загрузочные секторы диска.

Постоянное нахождение программ-«сторожей» в ОП существенно уменьшает ее объем, что является основным недостатком этих программ. К тому же программы-фильтры не способны «лечить» файлы или диски. Эту функцию выполняют другие антивирусные программы, например AVP, Norton Antivirus for Windows, Thunder Byte Professional, McAfee Virus Scan.

*Программы-ревизоры*являются надежным средством защиты от вирусов. Они запоминают исходное состояние программ, каталогов и системных областей диска при условии, что компьютер еще не был заражен вирусом. Впоследствии программа периодически сравнивает текущее состояние с исходным. При обнаружении несоответствий (по длине файла, дате модификации, коду циклического контроля файла) сообщение об этом появляется на экране компьютера. Среди программ-ревизоров можно выделить программу Adinf и дополнение к ней в виде Adinf cure Module.

*Программа-доктор*способна не только обнаруживать, но и «лечить» зараженные программы или диски. При этом она уничтожает зараженные программы тела вируса. Программы данного типа можно разделить на фаги и полифаги. *Фаги –*это программы, с помощью которых отыскиваются вирусы определенного вида. *Полифаги*предназначены для обнаружения и уничтожения большого числа разнообразных вирусов. В нашей стране наиболее часто используются такие полифаги, как MS Antivirus, Aidstest, Doctor Web. Они непрерывно обновляются для борьбы с появляющимися новыми вирусами.

*Программы-детекторы*способны обнаруживать файлы, зараженные одним или несколькими известными разработчикам программ вирусами.

*Программы-вакцины,*или *иммунизаторы,*относятся к классу резидентных программ. Они модифицируют программы и диски так, что это не отражается на их работе. Однако вирус, от которого производится вакцинация, считает их уже зараженными и не внедряется в них. В настоящий момент разработано множество антивирусных программ, получивших широкое признание и постоянно пополняющихся новыми средствами для борьбы с вирусами.

**5. Безопасность данных в интерактивной среде**

Интерактивные среды уязвимы с позиций безопасности данных. Примером интерактивных сред является любая из систем с коммуникационными возможностями, например электронная почта, компьютерные сети, Интернет.

С целью защиты информации от хулиганствующих элементов, неквалифицированных пользователей и преступников в системе Интернет применяется система полномочий, или управление доступом.

**Задание: Прочитать и сделать конспект ( выписать основные тезисы)**